

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-306001

(43)Date of publication of application : 02.11.2000

(51)Int.Cl.

G06F 17/60
G09C 1/00
G11B 20/10
H04L 9/32
// G06F 19/00

(21)Application number : 11-118618

(71)Applicant : SONY CORP

(22)Date of filing : 26.04.1999

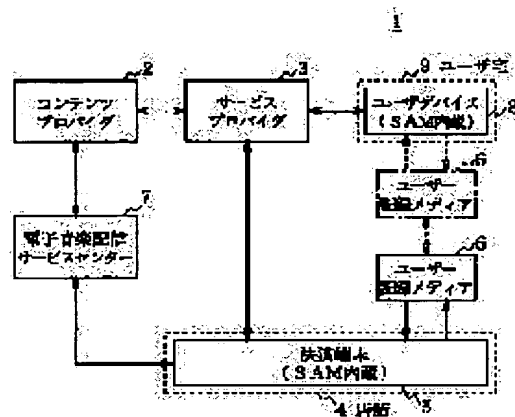
(72)Inventor : NAGAI KIKO

(54) DEVICE, METHOD, AND SYSTEM FOR DATA SETTLEMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To easily settle supplied provision data without any complicated procedure or operation by receiving money from a user and settling the account when a user device is authenticated according to user identification information.

SOLUTION: An electronic music distribution service center 7 decides that a user device 8 is already registered in the center 7 according to a specific public key. A settlement terminal 5 displays a music name of digital music contents and the value of its purchase on a monitor according to service condition information and charging information read out of its storage module. On the screen, a user selects the digital music contents and its value of the selected digital music contents is paid in cash or with a prepaid card or cash card through a prescribed throw-in hole. The settlement terminal 5 displays that on the monitor to inform the user.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

図1 電子音楽配信システムの全体構成

【特許請求の範囲】

【請求項1】所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取手段と、

上記読取手段によって読み取られた上記ユーザ識別情報に基づいて上記ユーザ機器を認証する認証手段と、

上記認証手段によって上記ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金を上記ユーザから受けて決済を行う決済手段とを具えることを特徴とするデータ決済装置。

【請求項2】上記データ決済装置は、上記認証手段によって上記ユーザ機器を認証したとき、上記提供データを上記記録媒体に記録するデータ記録手段を具えることを特徴とする請求項1に記載のデータ決済装置。

【請求項3】上記データ記録手段は、上記提供データを所定の方式で暗号化した後に上記記録媒体に記録することを特徴とする請求項2に記載のデータ決済装置。

【請求項4】上記データ決済装置は、上記提供データの供給条件に応じた販売履歴を所定の送信先へ送信する送信手段を具えることを特徴とする請求項1に記載のデータ決済装置。

【請求項5】上記決済手段は、上記認証手段によって上記ユーザを認証したとき、上記ユーザ機器と所定のデータ配信装置とがオンライン接続された状態で、上記データ配信装置から供給されて上記記録媒体に記録された上記提供データの再生履歴を上記供給条件として上記読取手段によって読み取り、上記再生履歴に基づいて上記提供データの再生回数に対応した上記対価の金額を所定の表示部に表示した後、上記金額の入金を受けて上記決済を行うことを特徴とする請求項1に記載のデータ決済装置。

【請求項6】上記決済手段は、上記提供データの再生回数に対応した上記対価を決済した後に上記記録媒体から上記再生履歴を削除することを特徴とする請求項5に記載のデータ決済装置。

【請求項7】所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取ステップと、上記読取ステップで読み取られた上記ユーザ識別情報に基づいて上記ユーザ機器を認証する認証ステップと、上記認証ステップで上記ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金を上記ユーザから受けて決済を行う決済ステップとを具えることを特徴とするデータ決済方法。

【請求項8】上記データ決済方法は、上記認証ステップで上記ユーザ機器を認証したとき、上記提供データを上記記録媒体に記録するデータ記録ステップを具えることを特徴とする請求項7に記載のデータ決済方法。

【請求項9】上記データ記録ステップは、上記提供データを所定の方式で暗号化した後に上記記録媒体に記録することを特徴とする請求項8に記載のデータ決済方法。

【請求項10】上記データ決済方法は、上記決済ステップに続いて、上記提供データの供給条件に応じた販売履歴を所定の送信先へ送信する送信ステップを具えることを特徴とする請求項7に記載のデータ決済方法。

【請求項11】上記決済ステップは、上記認証ステップによって上記ユーザを認証したとき、上記ユーザ機器と所定のデータ配信装置とがオンライン接続された状態で、上記データ配信装置から供給されて上記記録媒体に記録された上記提供データの再生履歴を上記供給条件として上記読取ステップで読み取り、上記再生履歴に基づいて上記提供データの再生回数に対応した上記対価の金額を所定の表示部に表示した後、上記金額の入金を受けて上記決済を行うことを特徴とする請求項7に記載のデータ決済方法。

【請求項12】上記決済ステップは、上記提供データの再生回数に対応した上記対価を決済した後に上記記録媒体から上記再生履歴を削除することを特徴とする請求項11に記載のデータ決済方法。

【請求項13】提供データを生成して提供するデータ提供装置、当該データ提供装置から供給された上記提供データを配信するデータ配信装置、当該データ配信装置によって配信された上記提供データの供給条件に対応した対価の入金を受けて決済を行うデータ決済装置、上記データ提供装置と上記データ配信装置と上記データ決済装置とを管理するデータ管理装置からなるデータ決済システムにおいて、

上記データ決済装置は、所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取手段と、

上記読取手段によって読み取られた上記ユーザ識別情報に基づいて上記ユーザ機器を認証する認証手段と、

上記認証手段によって上記ユーザ機器を認証したとき、ユーザに選択された所望の上記提供データの上記供給条件に対応した上記対価の入金を上記ユーザから受けて決済を行う決済手段とを具えることを特徴とするデータ決済システム。

【請求項14】上記データ決済装置は、上記認証手段によって上記ユーザ機器を認証したとき、上記提供データを上記記録媒体に記録するデータ記録手段を具えることを特徴とする請求項13に記載のデータ決済システム。

【請求項15】上記データ記録手段は、上記提供データを所定の方式で暗号化した後に上記記録媒体に記録することを特徴とする請求項14に記載のデータ決済システム。

【請求項16】上記データ決済装置は、上記提供データの供給条件に応じた販売履歴を上記データ管理装置へ送信する送信手段を具えることを特徴とする請求項13に記載のデータ決済システム。

【請求項17】上記データ決済装置の上記決済手段は、上記認証手段によって上記ユーザを認証したとき、上記ユーザ機器と上記データ配信装置とがオンライン接続された状態で、上記データ配信装置から供給されて上記記録媒体に記録された上記提供データの再生履歴を上記供給条件として上記読取手段によって読み取り、上記再生履歴に基づいて上記提供データの再生回数に対応した上記対価の金額を所定の表示部に表示した後、上記金額の入金を受けて上記決済を行うことを特徴とする請求項13に記載のデータ決済システム。

【請求項18】上記データ決済装置の上記決済手段は、上記提供データの再生回数に対応した上記対価を決済した後上記記録媒体から上記再生履歴を削除することを特徴とする請求項17に記載のデータ決済システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデータ決済装置、データ決済方法及びデータ決済システムに関し、例えば所望のデジタルコンテンツの決済を行うデータ決済装置、データ決済方法及びデータ決済システムに適用して好適なものである。

【0002】

【従来の技術】近年、インターネットによるコンピュータネットワークを用いて映画や音楽等のデジタルコンテンツを配信する情報提供サービスが始まっている。このような情報提供サービスの中で例えば電子音楽配信システムにおいては、レコード会社のようなコンテンツプロバイダによって作成されたデジタル音楽コンテンツを所定のサービスプロバイダからインターネット等のネットワークを介してオンラインでユーザ宅へ配信するようになされている。

【0003】ユーザ宅では、パーソナルコンピュータ等のユーザ機器によって受信したデジタル音楽コンテンツをユーザが選定したサービス条件（例えば買い切り又は再生可能回数等）の基で再生し、当該サービス条件の基で利用したコンテンツ利用履歴をユーザログとして記憶し、これを電子音楽配信サービスセンタへ送信する。

【0004】電子音楽配信サービスセンタは、送られてきたユーザログに基づいて利用料金を算出し、この利用料金をユーザに通知することにより、利用料金を例えばユーザの銀行口座上で決済するようになされている。

【0005】

【発明が解決しようとする課題】ところでかかる構成の電子音楽配信システムにおいて、電子音楽配信サービスセンタが利用料金を銀行口座上で決済するためには、予めユーザのクレジットカード番号や銀行口座番号を予め

保持しておく必要がある。

【0006】従ってユーザは、デジタル音楽コンテンツの配信を受けてその決済を行うために、クレジットカード番号や銀行口座番号をオンラインで電子音楽配信サービスセンタに送信するといった面倒な手続きを要する問題があった。

【0007】また電子音楽配信システムにおいては、電子音楽配信サービスセンタに直接オンラインで接続し得る機器をユーザが所有していなければ、デジタル音楽コンテンツの配信を受けることができず、誰でもが容易にデジタル音楽コンテンツの入手及び決済を実行し得ないという問題があった。

【0008】本発明は以上の点を考慮してなされたもので、供給される提供データの決済を煩雑な手続きや操作なしに容易に実行し得るデータ決済装置、データ決済方法及びデータ決済システムを提案しようとするものである。

【0009】

【課題を解決するための手段】かかる課題を解決するため本発明のデータ決済装置及びデータ決済方法においては、所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を記録媒体から読み取り、当該読み取られたユーザ識別情報に基づいてユーザ機器を認証し、当該ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金をユーザから受けて決済を行うようにする。

【0010】データ決済装置及びデータ決済方法では、記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限って、ユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができる。

【0011】また本発明のデータ決済システムにおいては、提供データを生成して提供するデータ提供装置、当該データ提供装置から供給された提供データを配信するデータ配信装置、当該データ配信装置によって配信された提供データの供給条件に対応した対価の入金を受けて決済を行うデータ決済装置、データ提供装置とデータ配信装置とデータ決済装置を管理するデータ管理装置からなるデータ決済システムにおいて、データ決済装置は、所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取手段と、当該読取手段によって読み取られたユーザ識別情報に基づいてユーザ機器を認証する認証手段と、当該認証手段によってユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金をユーザから受けて決済を行う決済手段とを設ける。

【0012】データ決済システムでは、データ決済装置によって記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限り、データ配信装置から配信されてユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができる。

【0013】

【発明の実施の形態】以下図面について、本発明の一実施の形態を詳述する。

【0014】(1) 電子音楽配信システムの全体構成
図1において、1は全体として本発明によるデータ決済システムとしての電子音楽配信システムを示し、ユーザに提供されるコンテンツとしては情報そのものが価値を有するデジタル音楽データを一例として以下説明を行う。

【0015】電子音楽配信システム1は、提供データとしてのデジタル音楽コンテンツを作成するデータ提供装置としてのコンテンツプロバイダ2と、当該コンテンツプロバイダ2によって作成されたデジタル音楽コンテンツを配信するデータ配信装置としてのサービスプロバイダ3と、当該サービスプロバイダ3から供給されたデジタル音楽コンテンツをフラッシュメモリカードでなるユーザ記録メディア6に書き込むと共に、その対価の支払いを受けて決済を行う店舗4に設置されたデータ決済装置としての決済端末5と、これら一連のデジタル音楽コンテンツの配信や決済に関する種々の管理を行うデータ管理装置としての電子音楽配信サービスセンタ7とから構成されている。

【0016】また電子音楽配信システム1は、サービスプロバイダ3とユーザ宅9に設置されている例えばパーソナルコンピュータ等のユーザデバイス8とをインターネット等のネットワーク（図示せず）を介してオンライン接続し、サービスプロバイダ3から供給されるデジタル音楽コンテンツをユーザ機器としてのユーザデバイス8を介してユーザ記録メディア6にダウンロードし得るようにもなされている。

【0017】(1-1) コンテンツプロバイダの構成
コンテンツプロバイダ2は、図2に示すようにコンテンツサーバ11に記憶しているユーザ供給用のデジタル音楽コンテンツD11を圧縮部12に送出する。圧縮部12は、例えばATRAC2(Adaptive Transform Acoustic Coding 2)（商標）と呼ばれる高能率符号化方式でデジタル音楽コンテンツD11を圧縮符号化し、これをデジタル音楽コンテンツD12として第1暗号化部13に送出する。

【0018】第1暗号化部13は、圧縮符号化されたデジタル音楽コンテンツD12に対して乱数発生部14から供給された所定ビット数の乱数をコンテンツキーK

coとして用いてDES(Data Encryption Standard)等の共通鍵暗号方式で暗号化し、これをコンテンツキーKcoによって暗号化されたデジタル音楽コンテンツD13としてセキュアコンテナ作成部17に送出する。

【0019】第2暗号化部15は、第1暗号化部13と同様に乱数発生部14からコンテンツキーKcoの供給を受け、電子音楽配信センタ7から供給された配送用キーKdを用いてコンテンツキーKcoをDES等の共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部17に送出する。

【0020】ポリシー記憶部16は、第1暗号化部13から供給されたデジタル音楽コンテンツD13の取扱方針（ポリシー）を記憶しており、デジタル音楽コンテンツD13に対応した取扱方針をセキュアコンテナ作成部17に送出する。

【0021】セキュアコンテナ作成部17は、図3に示すようにコンテンツキーKcoによって暗号化されたデジタル音楽コンテンツD13、配送用キーKdによって暗号化されたコンテンツキーKco、取扱方針、コンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13と暗号化されたコンテンツキーKcoと取扱方針とのハッシュ値に基づいて作成されたデジタル署名により構成されるコンテンツプロバイダセキュアコンテナD14を生成し、これをサービスプロバイダ3へ供給する。

【0022】相互認証部18は、電子音楽配信サービスセンタ7から配送用キーKdの供給を受けるのに先立って、デジタル署名を用いて電子音楽配信サービスセンタ7と相互認証し、またサービスプロバイダ3へのコンテンツプロバイダセキュアコンテナD14の供給に先立って、デジタル署名を用いてサービスプロバイダ3と相互認証する。

【0023】従って第2暗号化部15は、相互認証部18によって電子音楽配信サービスセンタ7との間で相互認証が得られると、電子音楽配信サービスセンタ7から配送用キーKdの供給を受ける。またセキュアコンテナ作成部17は、相互認証部18によってサービスプロバイダ3との間で相互認証が得られると、コンテンツプロバイダセキュアコンテナD14をサービスプロバイダ3へ供給する。

【0024】なおデジタル署名とは、送信者が例えば所定のメッセージを受信者に対して送信したとき、受信者の受け取ったメッセージが本当に送信者から送られてきたものなのか、あるいは送られてきたメッセージが何者かによって改ざんされていないか、という2つのことを確認し得るデータのことであり、送信すべきデータを基にハッシュ関数でハッシュ値をとり、これをコンテンツプロバイダ2における公開鍵暗号の秘密鍵Kscpで暗号化することにより作成される。

【0025】ハッシュ関数は、送信すべき所定のデータを入力として所定ビット長のデータに圧縮し、これをハ

ッシュ値として出力する関数である。このハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したときにハッシュ値の多くのビットが変化し、また同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有している。

【0026】デジタル署名と送信されたデータを受信した受信者は、デジタル署名を公開鍵暗号の公開鍵で復号してハッシュ値を得、さらに受信したデータのハッシュ値を算出して、当該算出したハッシュ値と公開鍵で復号したハッシュ値とを比較して等しいか否かを判定する。

【0027】このとき両者のハッシュ値が等しいと判定されたときには、受信したデータが改ざんされておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されてきたデータであることがわかる。なおデジタル署名のハッシュ関数としては、例えばSHA (Secure Hash Standard)-1が用いられる。

【0028】続いて、公開鍵暗号について具体的に説明

$$e d = 1 \mod L$$

【0032】が成立し、dはユークリッドの互除法で算出できる。このときnとeとが公開鍵とされ、p、q及びdが秘密鍵とされる。

$$C = M^e \mod n$$

【0035】を用いた処理によって算出される。

【0036】また暗号文Cは、次式

$$M = C^d \mod n$$

【0038】を用いた処理によって平文Mに復号される。

【0039】ここで証明については省略するが、RSA暗号で平文を暗号文に変換し、これを復号できるのは、

$$M = C^d = (M^e)^d = M^{(ed)} \mod n \quad \dots (4)$$

【0041】が成立するからである。

【0042】秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dを算出することはできるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは公開鍵eから秘密鍵dを算出することはできないので復号できない。以上のようにRSA暗号では、暗号化に使用する場合の鍵

$$y^2 = x^3 + ax + b$$

【0045】で示される楕円曲線上のある点をBとし、楕円曲線上の点Bがn回加算されたときの加算結果をnBと定義する共に、楕円曲線上の点Bがn回減算されたときの加算結果についても定義する。

【0046】この場合、BとnBとからnを算出するこ

$$C_1 = M + r n B$$

する。暗号化及び復号で同一の共通鍵を使用する共通鍵暗号方式に対して、公開鍵暗号方式は暗号化に使用する鍵と復号するときの鍵とがそれぞれ異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開してよい鍵は公開鍵と称され他方の秘密に保つ鍵は秘密鍵と称される。

【0029】このような公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を説明すると、まず2つの十分に大きな素数であるp及びqを求め、さらにpとqの積であるnを求める。そして(p-1)と(q-1)の最小公倍数Lを算出し、さらに3以上L未満でかつLと互いに素な数eを求める（すなわちeとLを共通に割り切れる数は、1のみである）。

【0030】次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわちd、e及びLの間には、次式

【0031】

【数1】

$$\dots (1)$$

【0033】暗号文Cは、平文Mから次式

【0034】

【数2】

$$\dots (2)$$

【0037】

【数3】

$$\dots (3)$$

フェルマーの小定理に根拠をおいており、次式

【0040】

【数4】

と復号する場合の鍵とを異なる鍵に設定することができ

る。

【0043】また、公開鍵暗号の他の例である楕円曲線暗号についても簡単に説明する。次式

【0044】

【数5】

$$\dots (5)$$

とは困難であることが証明されている。BとnBとを公開鍵としてnを秘密鍵とした場合、暗号文C₁及びC₂は乱数rを用いて平文Mから公開鍵で次式

【0047】

【数6】

$$\dots (6)$$

【0048】

$$C_2 = rB$$

【0049】を用いた処理によって算出される。

【0050】また暗号文 C_1 及び C_2 は、次式

$$M = C_1 - nC_2$$

【0052】を用いた処理によって平文 M に復号される。

【0053】このように復号できるのは、秘密鍵 n を有するものだけであり、以上のようにRSA暗号と同様に楕円曲線暗号でも暗号化に使用する場合の鍵と復号する場合の鍵とを異なる鍵に設定することができる。

【0054】(1-2) サービスプロバイダの構成
 サービスプロバイダ3は、図4に示すようにコンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナD14のうちコンテンツキー K_{co} で暗号化されたデジタル音楽コンテンツD13をコンテンツサーバ21に記憶した後、これをセキュアコンテナ作成部25に送出する。ここでコンテンツキー K_{co} は、配送用キー K_d によって暗号化されている状態である。

【0055】サービスプロバイダ3の値付け部22は、コンテンツプロバイダセキュアコンテナD14に含まれる取扱方針を基にデジタル音楽コンテンツD13に対するサービス条件(買い切り又は再生可能回数)に応じた価格情報を作成し、これをセキュアコンテナ作成部25に送出する。

【0056】因みにサービス条件の買い切りとは、ユーザ記録メディア6に記録されたデジタル音楽コンテンツD13をユーザ宅9のユーザデバイス8によって何度でも再生し得るデジタル音楽コンテンツD13の購入方法である。

【0057】またサービス条件の再生可能回数とは、サービスプロバイダ3とユーザ宅9のユーザデバイス8とをオンライン接続し、サービスプロバイダ3からユーザデバイス8を介してユーザ記録メディア6にダウンロードしたデジタル音楽コンテンツD13を、指定した再生可能回数の範囲内で再生し得るデジタル音楽コンテンツD13の購入方法である。

【0058】ポリシー記憶部23は、コンテンツプロバイダセキュアコンテナD14に含まれる取扱方針を記憶し、これをセキュアコンテナ作成部25に送出する。

【0059】セキュアコンテナ作成部25は、図5に示すようにコンテンツキー K_{co} で暗号化されたデジタル音楽コンテンツD13、配送用キー K_d で暗号化されたコンテンツキー K_{co} 、取扱方針、価格情報及びデジタル署名を含むサービスプロバイダセキュアコンテナD25を作成し、これを所定の通信インターフェース(図示せず)から専用のケーブルネットワーク、インターネット又は衛星放送等のネットワーク(図示せず)を介して決済端末5(図1)又はユーザ宅9のユーザデバイス8

【数7】

..... (7)

【0051】

【数8】

..... (8)

へオンラインで送信する。

【0060】この場合のデジタル署名とは、コンテンツキー K_{co} で暗号化されたデジタル音楽コンテンツD13、配送用キー K_d で暗号化されたコンテンツキー K_{co} 、取扱方針、及び価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3における公開鍵暗号の秘密鍵 K_{ssp} で暗号化したデータである。

【0061】相互認証部24は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナD14の供給を受けるのに先立って、デジタル署名を用いてコンテンツプロバイダ2と相互認証する。また相互認証部24は、決済端末5又はユーザデバイス8に対するサービスプロバイダセキュアコンテナD25の送信に先立って、デジタル署名を用いて決済端末5又はユーザデバイス8と相互認証する。

【0062】従ってコンテンツサーバ21は、相互認証部24によってコンテンツプロバイダ2との間で相互認証が得られると、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナD14の供給を受け、セキュアコンテナ作成部25は相互認証部24によって決済端末5又はユーザデバイス8との間で相互認証が得られると、決済端末5又はユーザデバイス8に対してサービスプロバイダセキュアコンテナD25を送信する。

【0063】(1-3) 決済端末の構成

決済端末5は、図6に示すようにサービスプロバイダ3(図1)や電子音楽配信センタ7(図1)とインターネット等のネットワークを介してデータ伝送を行う通信インターフェース31と、当該通信インターフェース31に接続されたSAM(Secure Application Module)32と、当該SAM32に接続されたハードディスクドライブ(HDD)33、液晶ディスプレイでなるモニタ34及びフラッシュメモリカードでなるユーザ記録メディア6とデータ交換を行うためのフラッシュメモリカードインターフェース35とから構成されている。

【0064】ここでSAMとは、電子音楽配信システム1の核をなすモジュールであり、決済処理、デジタル音楽コンテンツの著作権管理処理、配送用キー K_d の保持、コンテンツ再生履歴を表すユーザログの作成や削除等を実行するようになされており、決済端末5及びユーザ記録メディア6の記録再生機器であるユーザデバイス8(図1)にそれぞれ内蔵されている。

【0065】決済端末5に内蔵されたSAM32は、上述の機能に加えて電子音楽配信サービスセンタ7から伝

送された使用不許可SAMリスト（いわゆるブラックリスト）の保持、デジタル音楽コンテンツの販売履歴の生成及び保持機能を有している。

【0066】實際上SAM32は、動作する電圧又は周波数の幅が狭く外部からの不正なデータの読み出しが困難な（耐タンパー性）特性を持つシングルチップの暗号処理専用IC(Integrated Circuit)で構成され、相互認証モジュール41、課金処理モジュール42、記憶モジュール43及び復号／暗号化モジュール44を有している。なおユーザデバイス8においても、同様の構成のSAMが内蔵されている。

【0067】SAM32は、相互認証モジュール41によってサービスプロバイダ3から送られるデジタル署名に基づいて相互認証を実行し、又は電子音楽配信サービスセンタ7との間で「Authentication and Key Exchange(AKE) Protocol using Asymmetric Key Algorithm」と呼ばれる非対称鍵暗号技術を用いた相互認証を実行する。

【0068】非対称鍵暗号技術を用いた相互認証を実行するに当たって、例えば図7に示すように、決済端末5に内蔵されたSAM32の相互認証モジュール41は、

$$C1 = E_{\dots}(r1)$$

【0072】に示すような暗号文C1を生成し、これを電子音楽配信サービスセンタ7へ通信インターフェース31を介して送信する。

【0073】電子音楽配信サービスセンタ7は、電子音楽配信サービスセンタ7の秘密鍵 d_{esc} を用いた復号化

$$t1 = D_{\dots}(C1)$$

【0075】に示すような平文t1を求めた後、所定の乱数r2を生成してSAM32の公開鍵 e_{sam} を用いた暗号化関数 E_{sam} によって暗号化することにより、次式

$$C2 = E_{\dots}(r2)$$

【0077】に示すような暗号文C2を生成し、当該暗号文C2と平文t1とを決済端末5のSAM32へ送信する。

【0078】決済端末5のSAM32は、相互認証モジュール41によって乱数r1と電子音楽配信サービスセンタ7から送られてきた平文t1とが一致するか否かを検証し、一致したときには決済端末5が取り引きすべき

$$t2 = D_{\dots}(C2)$$

【0080】に示すような平文t2を求め、これを電子音楽配信サービスセンタ7へ送信する。

【0081】電子音楽配信サービスセンタ7は、乱数r2と決済端末5のSAM32から送られてきた平文t2とが一致するか否かを検証し、一致したときには電子音楽配信サービスセンタ7が取り引きすべき正当な決済端末5であることを認証し得、すなわち相互認証が完了する。

$$S = E_{\dots}(Ks)$$

予め電子音楽配信サービスセンタ7の公開鍵 e_{esc} 、SAM32の秘密鍵 d_{sam} 及びSAM32の公開鍵 e_{sam} を記憶しており、また電子音楽配信サービスセンタ7は当該電子音楽配信サービスセンタ7の公開鍵 e_{esc} 、電子音楽配信サービスセンタ7の秘密鍵 d_{esc} 、電子音楽配信サービスセンタ7に予め登録された決済端末5におけるSAM32の公開鍵 e_{sam} を予め記憶している。

【0069】尚、ここではSAM32の公開鍵 e_{sam} を用いた暗号化関数を E_{sam} とし、SAM32の秘密鍵 d_{sam} を用いた復号化関数を D_{sam} とする。また電子音楽配信サービスセンタ7の公開鍵 e_{esc} を用いた暗号化関数を E_{esc} とし、電子音楽配信サービスセンタ7の秘密鍵 d_{esc} を用いた復号化関数を D_{esc} とする。

【0070】この場合決済端末5のSAM32は、相互認証モジュール41によって所定の乱数r1を生成し、当該乱数r1を電子音楽配信サービスセンタ7の公開鍵 e_{esc} を用いた暗号化関数 E_{esc} によって暗号化することにより、次式

【0071】

【数9】

..... (9)

関数 D_{esc} によって暗号文C1を復号することにより、次式

【0074】

【数10】

..... (10)

【0076】

【数11】

..... (11)

正当な電子音楽配信サービスセンタ7であることを認証し得、このときSAM32の秘密鍵 d_{sam} を用いた復号化関数 D_{sam} によって暗号文C2を復号することにより、次式

【0079】

【数12】

..... (12)

【0082】電子音楽配信サービスセンタ7は、相互認証が完了したので電子音楽配信サービスセンタ7と決済端末5との間で使用する共通鍵としてセッションキーKsを生成し、これをSAM32の公開鍵 e_{sam} を用いた暗号化関数 E_{sam} によって暗号化することにより、次式

【0083】

【数13】

..... (13)

【0084】に示すような暗号文Sを生成し、これを決済端末5のSAM32へ送信する。

【0085】決済端末5のSAM32は、相互認証モジュール41によって電子音楽配信サービスセンタ7から送られてきた暗号文SをSAM32の秘密鍵 d_{sam} を用

$$Ks = D_{..n} (S)$$

【0087】に示すようなセッションキーKsを求める。

【0088】これにより決済端末5は、以後電子音楽配信サービスセンタ7との間でデータ伝送を行う場合にセッションキーKsで暗号化するようになされている。これにより決済端末5と電子音楽配信サービスセンタ7との間で行われるデータ伝送のセキュリティを保証する。

【0089】かくして電子音楽配信サービスセンタ7は、セッションキーKsに基づいて配送用キーKd及び使用不許可SAMリスト（ブラックリスト）を暗号化して安全に決済端末5のSAM32へデータ伝送し得るようになされている。

【0090】決済端末5は、SAM32の相互認証モジュール41によって電子音楽配信サービスセンタ7との相互認証が済むと、電子音楽配信サービスセンタ7から送られてきた配送用キーKd及び使用不許可SAMリストをSAM32の記憶モジュール43に記憶する。

【0091】また決済端末5は、SAM32の相互認証モジュール41によってサービスプロバイダ3との相互認証が済むと、通信インターフェース31を介してサービスプロバイダ3からサービスプロバイダセキュアコンテナD25を取り込み、そのうちの取扱情報及び価格情報に基づいてサービス条件情報及び課金情報を生成し、これらを記憶モジュール43に格納する。

【0092】このとき同時に決済端末5は、サービスプロバイダセキュアコンテナD25のうちコンテンツキーKcoによって暗号化されたデジタル音楽コンテンツD13をハードディスクドライブ33に格納する。なお、このデジタル音楽コンテンツD13のコンテンツキーKcoは、配送用キーKdによって暗号化された状態である。

【0093】そして決済端末5は、ユーザによって持ち込まれたユーザ記録メディア6がカードスロット50Aを介して装着されて読取手段としてのフラッシュメモリカードインターフェース50に接続されると、当該フラッシュメモリカードインターフェース50によってユーザ記録メディア6の所定記憶領域に格納されている公開鍵証明書を読み出し、これを記憶モジュール43に格納する。

【0094】ここで公開鍵証明書とは、電子音楽配信サービスセンタ7から発行されたデータで、ユーザデバイス8の出荷時に内蔵されたSAMに予め保持されており、SAM公開鍵KpubとSAMのID (Identification) 番号であるSAMIDとを含み、ユーザデバイス8に

いた復号化関数 D_{sam} を用いて復号することにより、次式

【0086】

【数14】

..... (14)

よってユーザ記録メディア6の所定記憶領域に記録されている。

【0095】決済端末5は、記憶モジュール43に格納されたSAM公開鍵Kpubを読み出して通信インターフェース31を介して電子音楽配信サービスセンタ7へ送信する。

【0096】電子音楽配信サービスセンタ7は、SAM公開鍵Kpubに基づいてユーザデバイス8が電子音楽配信サービスセンタ7に予め登録されたものであることを判別し、この結果を決済端末5へ通知する。

【0097】決済端末5は、電子音楽配信サービスセンタ7からユーザデバイス8が正規ユーザのものであることを通知してもらうと、認証手段としての相互認証モジュール42により記憶モジュール43に格納されているSAMIDと使用不許可SAMリスト（ブラックリスト）とを比較して、SAMIDが使用不許可SAMリストに記載されているか否かを判別する。

【0098】ここで決済端末5は、相互認証モジュール42によりユーザデバイス8が正規ユーザのものであり、かつブラックリストに記載されていないことを認識すると、GUI (Graphical User Interface) 生成モジュール51にGUI画面の生成を指示する。

【0099】GUI生成モジュール51は、記憶モジュール43から読み出したサービス条件情報及び課金情報に基づいてデジタル音楽コンテンツの曲名を表したGUI画面及び買い切りの対価を表したGUI画面を生成し、これらをモニタ34に表示する。

【0100】GUI生成モジュール51は、モニタ34に表示されたGUI画面上でユーザによりデジタル音楽コンテンツが選択され、当該選択されたデジタル音楽コンテンツの対価が所定の現金投入口やカード投入口を介して現金、プリペイドカード又はキャッシュカード等のいずれかによって支払われたことを確認すると、その旨を決済手段としての課金処理モジュール42に通知する。

【0101】課金処理モジュール42は、選択されたデジタル音楽コンテンツにおける買い切りの対価の支払いによりデジタル音楽コンテンツの決済を行って決済処理が終了すると、その旨を復号／暗号化モジュール44に対して通知する。

【0102】復号／暗号化モジュール44は、復号ユニット45、暗号化ユニット46及び記録ユニット47によって構成され、決済終了の通知を課金処理モジュール42から受けると、復号ユニット45によってハードデ

ィスクドライブ33からコンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13を読み出すと共に、記憶モジュール43から読み出した配送用キーKdでデジタル音楽コンテンツD13のコンテンツキーKcoを復号して暗号化ユニット47に送出する。

【0103】暗号化ユニット47は、配送用キーKdで復号されたコンテンツキーKcoを記憶モジュール43から読み出した公開鍵証明書のSAM公開鍵Kpubで再度暗号化し、当該SAM公開鍵Kpubで暗号化されたコンテンツキーKcoとコンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13とを、データ記録手段としての記録ユニット48によってフラッシュメモリカードインターフェース50を介してユーザ記録メディア6に書き込むと共に、書き込み終了したことをGUI生成モジュール51に通知する。

【0104】GUI生成モジュール51は、コンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13及びSAM公開鍵Kpubで暗号化されたコンテンツキーKcoのユーザ記録メディア6に対する書き込みが終了した旨を表したGUI画面を生成し、これをモニタ34に表示してユーザへ通知する。これにより決済端末5は、買い取りで購入されたデジタル音楽コンテンツのユーザ記録メディア6に対する書き込み及びその決済を終了する。

【0105】この結果、ユーザ記録メディア6にはコンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13と、SAM公開鍵Kpubによって暗号化されたコンテンツキーKcoとが記録される。

【0106】ユーザ宅9に設置されたユーザデバイス8は、デジタル音楽コンテンツの記録されたユーザ記録メディア6が装填されると、内蔵されたSAMによりSAM公開鍵Kpubに対応したSAM秘密鍵でコンテンツキーKcoを復号し、当該復号したコンテンツキーKcoでデジタル音楽コンテンツD13を復号することにより再生データを生成し、これをスピーカ（図示せず）を介して出力する。

【0107】ところで復号ユニット45は、ユーザによって選定されたデジタル音楽コンテンツD13のコンテンツキーKcoを配送用キーKdで復号したときには、その旨を課金処理モジュール42に通知する。

【0108】このとき課金処理モジュール42は、配送用キーKdでコンテンツキーKcoを復号した旨の通知を受ける度にコンテンツ再生履歴を表すユーザログを生成すると共に、買い取りで購入されたデジタル音楽コンテンツD13の販売履歴（顧客情報やデジタル音楽コンテンツの種類を表すコンテンツ情報）を生成して記憶モジュール43に保存する。

【0109】そして決済端末5は、相互認証モジュール41により電子音楽配信サービスセンタ7との間で非対称鍵暗号技術を用いて相互認証を行った後に、課金処理

モジュール42により記憶モジュール43からユーザログ及び販売履歴を読み出し、当該ユーザログ及び販売履歴をセッションキーKsで暗号化した後に送信手段としての通信インターフェース31を介して電子音楽配信サービスセンタ7へ送信する。

【0110】かくして電子音楽配信サービスセンタ7は、決済端末5から送られてきたユーザログ及び販売履歴に基づいてデジタル音楽コンテンツの再生履歴や、ユーザのデジタル音楽コンテンツの販売状況を調査し得るようになされている。

【0111】（2）買い取りでデジタル音楽コンテンツをオフライン購入するときの決済シーケンス
続いて、電子音楽配信システム1において買い取りでデジタル音楽コンテンツをオフライン購入するときの決済シーケンスについて、図8を用いて説明する。

【0112】まず第1ステップ（SP）として、決済端末5は電子音楽配信サービスセンタ7との間で非対称鍵暗号技術を用いた相互認証（図7）を実行し、電子音楽配信サービスセンタ7からセッションキーKsで暗号化された配送用キーKd及び使用不許可SAMリスト（ブラックリスト）の供給を受ける。

【0113】第2ステップとして、決済端末5は、サービスプロバイダ3との間でデジタル署名を用いて相互認証を実行した後、サービスプロバイダ3からサービスプロバイダセキュアコンテナD25の供給を受け、そのうちコンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13と、配送用キーKdで暗号化されたコンテンツキーKcoをハードディスクドライブ33に格納する。

【0114】第3ステップとして、決済端末5はユーザによってカードスロット50Aにユーザ記録メディア6が装着され、フラッシュメモリカードインターフェース50を介してユーザ記録メディア6の所定記憶領域から公開鍵証明書のSAM公開鍵Kpub及びSAMIDを読み出してSAM32の記憶モジュール43に格納する。

【0115】第4ステップとして、決済端末5はSAM公開鍵Kpubに基づいてユーザデバイス8が正規ユーザであることを電子音楽配信サービスセンタ7から通知された後、SAMIDに基づいてブラックリストに記載されたユーザでないことを確認すると、モニタ34にデジタル音楽コンテンツの曲名を表したGUI画面を表示する。

【0116】第5ステップとして、決済端末5はGUI画面上におけるユーザ操作によって選定されたデジタル音楽コンテンツを判別し、第6ステップとして、選定されたデジタル音楽コンテンツの利用料金を表したGUI画面をモニタ34に表示する。

【0117】第7ステップとして、決済端末5はモニタ34のGUI画面上に表示された利用料金の入金処理がユーザによって完了したことをSAM32の課金処理モ

ジュール4 2によって確認する。

【0118】第8ステップとして、決済端末5は復号／暗号化モジュール4 4によってデジタル音楽コンテンツD 1 3のコンテンツキーKcoを配送用キーKdで復号し、当該復号したコンテンツキーKcoをSAM公開鍵Kpubで再度暗号化し、当該SAM公開鍵Kpubで暗号化されたコンテンツキーKcoと、コンテンツキーKcoで暗号化されたデジタル音楽コンテンツD 1 3とをユーザ記録メディア6に書き込む。

【0119】第9ステップとして、決済端末5は復号／暗号化モジュール4 4によって配送用キーKdでコンテンツキーKcoを復号したときに課金処理モジュール4 2によってユーザログを生成すると共に、買い取り購入されたデジタル音楽コンテンツD 1 3の販売履歴（顧客情報やデジタル音楽コンテンツの種類を表すコンテンツ情報）を生成して記憶モジュール4 3に保存する。

【0120】第10ステップとして、決済端末5は相互認証モジュール4 1により電子音楽配信サービスセンタ7との間で相互認証を行った後、第11に、課金処理モジュール4 2により記憶モジュール4 3からユーザログ及び販売履歴を読み出し、当該販売履歴をセッションキーKsで暗号化した後に通信インターフェース3 1を介して電子音楽配信サービスセンタ7へ送信する。

【0121】(3) デジタル音楽コンテンツをオンライン購入するときのユーザログを用いた決済シーケンス次に、電子音楽配信システム1（図1）においてサービスプロバイダ3とユーザ宅9のユーザデバイス8とがインターネット等のネットワークを介してオンライン接続された状態で、サービスプロバイダ3に対して所望のデジタル音楽コンテンツを指定し、サービスプロバイダ3から供給される所望のデジタル音楽コンテンツをユーザデバイス8を介してユーザ記録メディア6に書き込み、当該ユーザ記録メディア6に書き込まれたデジタル音楽コンテンツを再生したときに再生回数分の利用料金を支払う決済シーケンスを、図9を用いて説明する。

【0122】ここでユーザ記録メディア6には、ユーザデバイス8の内蔵SAMによってデジタル音楽コンテンツの再生回数に応じたユーザログが所定記憶領域に記録され、かくして決済端末5はユーザ記録メディア6からユーザログを読み出し、当該読み出したユーザログに基づいて利用料金を決済するようになされている。

【0123】まず第1ステップ（SP）として、決済端末5はユーザによって持参されたユーザ記録メディア6がカードスロット5 0 Aに装着されることにより、ユーザ記録メディア6の所定記憶領域に記録されたユーザログ及び公開鍵証明書を読み出す。なおユーザログは、楕円曲線暗号によってデジタル署名されており、改ざんされないように暗号化されている。

【0124】第2ステップとして、決済端末5は電子音楽配信サービスセンタ7との間で非対称鍵暗号技術を用

いた相互認証を実行し、電子音楽配信サービスセンタ7からセッションキーKsで暗号化された配送用キーKd及び使用不許可SAMリスト（ブラックリスト）の供給を受ける。

【0125】このとき決済端末5は、公開鍵証明書に含まれているSAM公開鍵Kpubに基づいてユーザデバイス8が正規ユーザのものであることを電子音楽配信サービスセンタ7から通知され、公開鍵証明書に含まれているSAM IDに基づいて使用不許可SAMリストに記載されたユーザではないことを確認すると、ユーザログを読み取ると共に当該ユーザログを読み取ったことを表す確認フラグを立てる。これによりユーザ記録メディア6には、確認フラグが立てられたので、決済端末5のカードスロット5 0 Aに再度装着されたときにユーザログが再度読み取られることがなく、利用料金の支払い請求を2度受けずに済む。

【0126】第3ステップとして、決済端末5はユーザ記録メディア6から読み出したユーザログ及び公開鍵証明書を電子音楽配信サービスセンタ7に対してインターネット等のネットワークを介して送信する。これにより電子音楽配信サービスセンタ7は、ユーザログに基づいて再生回数に応じた利用料金を算出し、ユーザに対する請求金額情報をネットワークを介して決済端末5へ送信する。

【0127】第4ステップとして、決済端末5は電子音楽配信サービスセンタ7から送られてきた利用料金の請求金額情報を受信し、GUI生成モジュール5 1によって請求金額情報に基づく利用料金を表したGUI画面を生成する。

【0128】第5ステップとして、決済端末5は請求金額情報に基づく利用料金を表したGUI画面をモニタ3 4に表示してユーザに通知する。ユーザは、モニタ3 4に表示されたGUI画面を確認することにより、再生回数に応じた利用料金の金額を認識し得る。

【0129】第6ステップとして、決済端末5はユーザによって利用料金の入金処理が完了したことを確認すると、第7ステップとして課金処理モジュール4 2により入金処理完了情報を通信インターフェース3 1を介して電子音楽配信サービスセンタ7へ送信する。

【0130】電子音楽配信サービスセンタ7は、入金処理完了情報を受け取るとユーザログに基づく再生回数に応じた利用料金の決済が終了したので、公開鍵証明書のSAM公開鍵Kpubで暗号化したユーザログ削除許可証を生成し、これを決済端末5へ送信する。

【0131】第8ステップとして、決済端末5は電子音楽配信サービスセンタ7からSAM公開鍵Kpubで暗号化されたユーザログ削除許可証を受信する。第9に、決済端末5は電子音楽配信サービスセンタ7から受信したユーザログ削除許可証をSAM公開鍵Kpubに対応したSAM秘密鍵で復号して、当該復号したユーザログ削除

許可証に基づいてユーザログを削除する。

【0132】ここで決済端末5は、ユーザログ削除許可証に基づいてユーザログを削除する場合、確認フラグが立っていることを確認したときにユーザログを削除するようになされている。これによりユーザ記録メディア6は、所定記憶領域に記録されたユーザログが削除され、再生回数分の利用料金の決済が全て終了する。

【0133】(4)実施の形態における動作及び効果以上の構成において、電子音楽配信システム1の店舗4に設置されている決済端末5は、ユーザが買い取りでデジタル音楽コンテンツをオフライン購入する場合、まず電子音楽配信サービスセンタ7との間で相互認証を実行した後に配送用キーKd及び使用不許可SAMリストの供給を受ける。

【0134】次に決済端末5は、サービスプロバイダ3との間で相互認証を実行した後にサービスプロバイダ3から供給されるコンテンツキーKcoで暗号化されたデジタル音楽コンテンツD13と、配送用キーKdで暗号化されたコンテンツキーKcoとをハードディスクドライブ33に予め記憶しておく。

【0135】ユーザデバイス8は、内蔵SAMによってユーザ記録メディア6の所定記憶領域に公開鍵証明書を記録し、ユーザは公開鍵証明書の記録されたユーザ記録メディア6を持参して店舗5に設置された決済端末5のカードスロット50Aにユーザ記録メディア6を装着する。

【0136】そして決済端末5は、ユーザによってカードスロット50Aに装着されたユーザ記録メディア6から公開鍵証明書のSAM公開鍵Kpub及びSAMIDを読み出し、ユーザデバイス8がブラックリストに記載されていない正規ユーザであることを確認すると、デジタル音楽コンテンツの曲名及び買い切りの対価を表したGUI画面をモニタ34に表示する。

【0137】続いて決済端末5は、ユーザによってデジタル音楽コンテンツの曲名が選定され、その利用料金の入金処理が完了したことを確認すると、配送用キーKdでコンテンツキーKcoを復号すると共にユーザログを生成し、SAM公開鍵KpubでコンテンツキーKcoを再度暗号化した後、当該SAM公開鍵Kpubで再度暗号化されたコンテンツキーKcoと、コンテンツキーKcoで暗号化されているデジタル音楽コンテンツD13とをユーザ記録メディア6に書き込む。

【0138】最後に決済端末5は、生成したユーザログと共にデジタル音楽コンテンツの販売履歴を電子音楽配信サービスセンタ7へ送信し、デジタル音楽コンテンツをオフライン購入したときの決済処理を終了する。

【0139】また決済端末5は、ユーザがデジタル音楽コンテンツをサービスプロバイダ3からオンライン購入する場合、ユーザによって持参されたユーザ記録メディア6がカードスロット50Aに装填されると、ユーザ

記録メディア6から再生回数に応じて記録されたユーザログ及び公開鍵証明書を読み出し、そのうちの公開鍵証明書に基づいてユーザデバイス8が正規ユーザのものであることを確認する。

【0140】そして決済端末5は、記録メディア6から読み出したユーザログ及び公開鍵証明書を電子音楽配信サービスセンタ7に対してインターネット等のネットワークを介して送信する。これにより電子音楽配信サービスセンタ7は、ユーザログに基づいて再生回数に応じた利用料金を算出し、ユーザに対する請求金額情報をネットワークを介して決済端末5へ送信する。

【0141】続いて決済端末5は、電子音楽配信サービスセンタ7から送られてきた利用料金の請求金額情報に基づく利用料金を表したGUI画面をモニタ34に表示し、ユーザによって利用料金の入金処理が完了したことを確認すると、入金処理完了情報を電子音楽配信サービスセンタ7へ送信する。

【0142】これにより電子音楽配信サービスセンタ7は、入金処理完了情報を受け取るとユーザ記録メディア6に記録されたユーザログの決済が終了したので、公開鍵証明書のSAM公開鍵Kpubで暗号化したユーザログ削除許可証を決済端末5へ送信する。

【0143】最後に決済端末5は、電子音楽配信サービスセンタ7から送られてきたユーザログ削除許可証をSAM秘密鍵で復号し、当該復号したユーザログ削除許可証に基づいてユーザログを削除した後にユーザ記録メディア6をユーザへ返却し、デジタル音楽コンテンツをサービスプロバイダ3からオンライン購入したときの決済処理を終了する。

【0144】このように決済端末5は、デジタル音楽コンテンツをオフライン購入又はオンライン購入する場合においても、ユーザ記録メディア6から公開鍵証明書のSAM公開鍵Kpub及びSAMIDを読み出し、当該SAM公開鍵Kpub及びSAMIDに基づいてユーザデバイス8を認証する。

【0145】そして決済端末5は、ユーザデバイス8が正規ユーザのものであることを確認した場合にだけ、ユーザによって選定されたデジタル音楽コンテンツをユーザ記録メディア6に書き込むことにより、SAM内蔵のユーザデバイス8を所有している正規ユーザに対してのみデジタル音楽コンテンツを供給することができる。

【0146】同時に決済端末5は、デジタル音楽コンテンツを供給する際にユーザデバイス8毎に設定されたSAM公開鍵KpubでコンテンツキーKcoをさらに暗号化しているので、SAM公開鍵Kpubに対応したSAM秘密鍵を保持するSAM内蔵のユーザデバイス8によってのみコンテンツキーKcoを復号してデジタル音楽コンテンツを再生することができる。

【0147】すなわち電子音楽配信システム1では、デ

ィジタル音楽コンテンツの記録されたユーザ記録メディア6を他人の所有するユーザデバイスで再生することはできず、かくしてィジタル音楽コンテンツの著作権を有益に保護することができる。

【0148】また決済端末5は、ユーザデバイス8が正規ユーザのものであることを確認したときにィジタル音楽コンテンツの買い切りの対価又は再生回数に応じた利用料金を表したG U I画面をモニタ34に表示し、ユーザによって現金、プリペイドカード又はキャッシュカード等のいずれかによって入金処理が実行されるようになされており、これにより、ユーザに対して自分自身を証明するクレジット番号等を入力する等の煩雑な手続きを強いることなく決済を完了することができる。

【0149】かくして電子音楽配信システム1では、サービスプロバイダ3とオンライン接続し得るユーザデバイス8を所有しないユーザであっても、SAMを内蔵したポータブル機器やカーオーディオ等を所有してさえいれば、店舗4に設置されている決済端末5を介して所望のィジタル音楽コンテンツをオフライン購入し得ると共に、その場で現金、プリペイドカード又はキャッシュカード等のいずれかによって容易に決済することができる。

【0150】またユーザは、ユーザデバイス8とサービスプロバイダ3とをオンライン接続して所望のィジタル音楽コンテンツをオンライン購入した場合でも、内蔵SAMによってユーザログの記録されたユーザ記録メディア6を店舗4へ持参して決済端末5へ装着し、当該決済端末5によって指示された再生回数に応じた利用料金をその場で容易に決済することができる。

【0151】かくしてユーザは、電子音楽配信サービスセンタ7に対して自分自信を証明するクレジットカード番号等をオンラインで送信する必要がないので面倒な手続きなしに決済することができる。

【0152】さらに決済端末5では、サービスプロバイダ3から予めィジタル音楽コンテンツをダウンロードしてハードディスクドライブ33に格納しておくことにより、オフライン購入する場合にユーザ記録メディア6に対してダウンロードに要する時間が不要になり、決済端末5のデータ転送速度でユーザ記録メディア6にィジタル音楽コンテンツを書き込むことができ、かくして買い取りでオフライン購入するユーザに対して購入時の待ち時間を大幅に短縮することができる。

【0153】さらに電子音楽配信システム1は、ユーザログと共に販売履歴を決済端末5から電子音楽配信サービスセンタ7へ送信するようにしたことにより、当該電子音楽配信サービスセンタ7によってィジタル音楽コンテンツのマーケティングリサーチを容易に実行することができる。

【0154】以上の構成によれば、電子音楽配信システム1はィジタル音楽コンテンツをオンライン購入又は

オフライン購入する場合、ユーザ記録メディア6から読み出した公開鍵証明書に基づいてユーザデバイス8が正規ユーザのものであることを確認したとき、オフライン又はオンラインによるィジタル音楽コンテンツの供給条件に対応した対価の入金を受けて決済するようにしたことにより、自分自信を証明するクレジットカード番号等の面倒な入力手続きを正規ユーザに対して強いることなく容易に決済することができる。

【0155】(5) 他の実施の形態

なお上述の実施の形態においては、提供データとしてィジタル音楽コンテンツを提供するようにした場合について述べたが、本発明はこれに限らず、映画やゲーム又はアプリケーションソフトウェア等の種々のィジタルデータを提供するようにしても良い。この場合にも、上述の実施の形態と同様の効果を得ることができる。

【0156】また上述の実施の形態においては、電子音楽配信サービスセンタ7とコンテンツプロバイダ2、コンテンツプロバイダ2とサービスプロバイダ3、サービスプロバイダ3と決済端末5との間をオンライン接続してデータ伝送するようにした場合について述べたが、本発明はこれに限らず、オフラインでデータを供給するようにしても良い。

【0157】さらに上述の実施の形態においては、ユーザがィジタル音楽コンテンツを買い取りでオフライン購入するようにした場合について述べたが、本発明はこれに限らず、オフラインで指定した再生可能回数でィジタル音楽コンテンツを購入し、再生回数に応じて記録されたユーザログに基づいて決済端末5で決済するようにしても良い。この場合、ユーザ記録メディア6にィジタル音楽コンテンツを記録するときに決済を行うのではなく、ユーザデバイス8によってユーザ記録メディア6に記録されたユーザログを決済端末5に再度読み取らせることにより決済を行う。

【0158】さらに上述の実施の形態においては、記録媒体であるユーザ記録メディア6としてフラッシュメモリカードを記録媒体として用いるようにした場合について述べたが、本発明はこれに限らず、光磁気ディスク等の他の種々の記録媒体を用いるようにしても良い。

【0159】さらに上述の実施の形態においては、ユーザがィジタル音楽コンテンツをサービスプロバイダ3からオンライン購入したとき、ユーザデバイス8によって再生回数に応じたユーザログをユーザ記録メディア6に記録し、当該ユーザ記録メディア6を介して決済端末5に直接ユーザログを読み取らせ、当該決済端末5から電子音楽配信サービスセンタ7へユーザログを送信するようにした場合について述べたが、本発明はこれに限らず、ユーザデバイス8の内蔵SAMが生成したユーザログをサービスプロバイダ3へオンラインで直接送信するようにしても良い。この場合、ユーザデバイス8はユーザログを送信し終わったことを示す確認フラグを立て、

再度送信することを防止する。

【0160】さらに上述の実施の形態においては、決済端末5がモニタ34にデジタル音楽コンテンツの曲名や利用料金だけを表示するようにした場合について述べたが、本発明はこれに限らず、曲名のラベルプリント機能や、デジタル音楽コンテンツの試聴機能、さらにアーティストの顔写真を表示した静止画像をモニタ34に表示する表示機能等の種々の付加機能を設定するようにしても良い。

【0161】

【発明の効果】 上述のように本発明によれば、記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限り、ユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができ、かくして供給される提供データの決済を煩雑な手続きなしに容易に実行し得るデータ決済装置及びデータ決済方法を実現できる。

【0162】 また本発明によれば、記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限り、データ配信装置から配信されてユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができ、かくして供給される提供データの決済をデータ決済装置によって煩雑な手続きなしに容易に実行し得るデータ決済システムを実現できる。

【図面の簡単な説明】

【図1】 本発明による電子音楽配信システムの全体構成を示すブロック図である。

【図2】 コンテンツプロバイダの構成を示すブロック図である。

【図3】 コンテンツプロバイダセキュアコンテナのデータ構造を示す略線図である。

【図4】 サービスプロバイダの構成を示すブロック図である。

【図5】 サービスプロバイダセキュアコンテナのデータ構造を示す略線図である。

【図6】 決済端末の構成を示すブロック図である。

【図7】 決済端末と電子音楽配信サービスセンタとの間における相互認証の処理シーケンスを示す略線図である。

【図8】 買い取りでデジタル音楽コンテンツをオフライン購入するときの決済シーケンスを示す略線図である。

【図9】 デジタル音楽コンテンツをオンライン購入するときのユーザログを用いた決済シーケンスを示す略線図である。

【符号の説明】

1……電子音楽配信システム、2……コンテンツプロバイダ、3……サービスプロバイダ、5……決済端末、6……ユーザ記録メディア、7……電子音楽配信サービスセンタ、8……ユーザデバイス、32……SAM、33……HDD、34……モニタ、41……相互認証モジュール、42……課金処理モジュール、43……記憶モジュール、44……復号/暗号化モジュール、45……復号ユニット、46……暗号化ユニット、47……記録ユニット、50……フラッシュメモリカードインターフェース、51……GUI生成モジュール。

【図1】

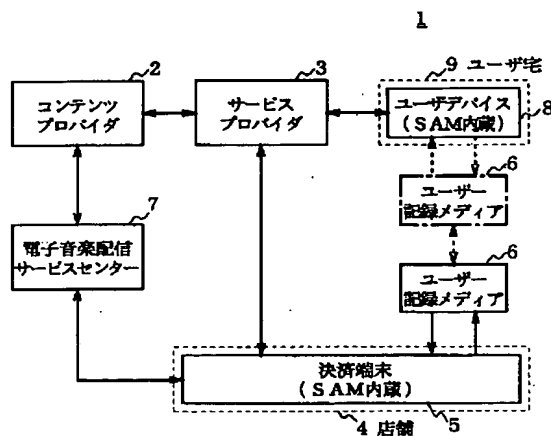


図1 電子音楽配信システムの全体構成

【図4】

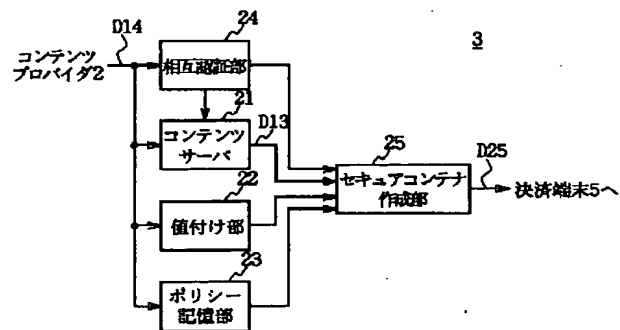


図4 サービスプロバイダの構成

【図 2】

2

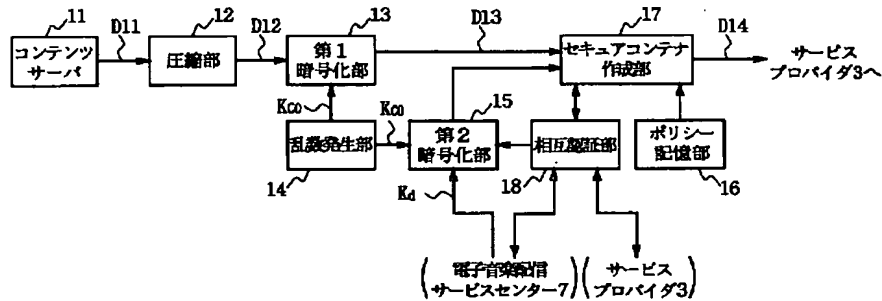


図2 コンテンツプロバイダの構成

【図 3】

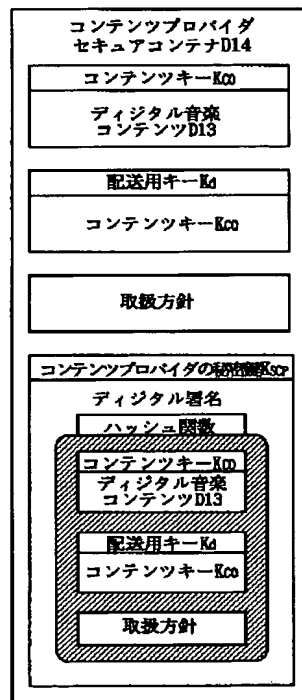


図3 コンテンツプロバイダセキュアコンテンツのデータ構造

【図 5】

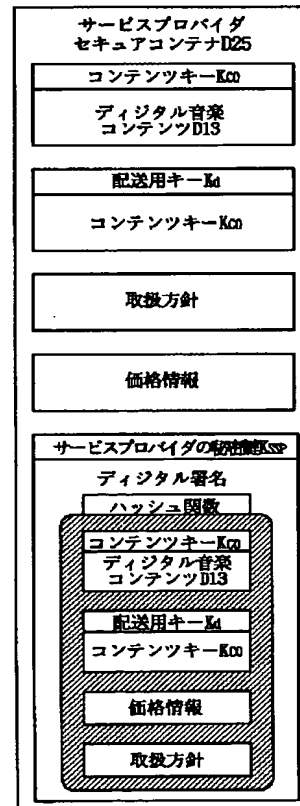


図5 サービスプロバイダセキュアコンテンツのデータ構造

【図6】

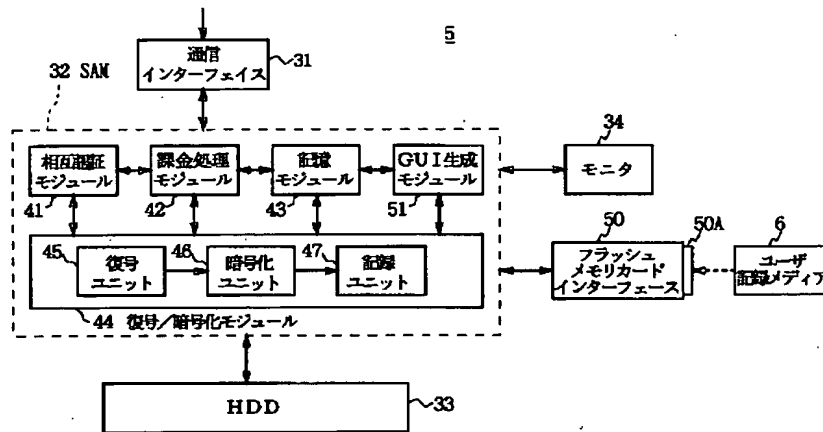


図6 決済端末の構成

【図7】

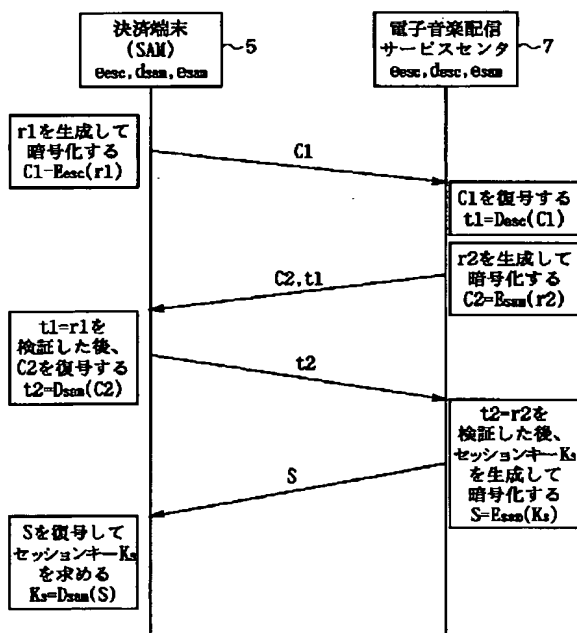


図7 決済端末と電子音楽配信サービスセンタとの間における相互認証の処理シーケンス

【図8】

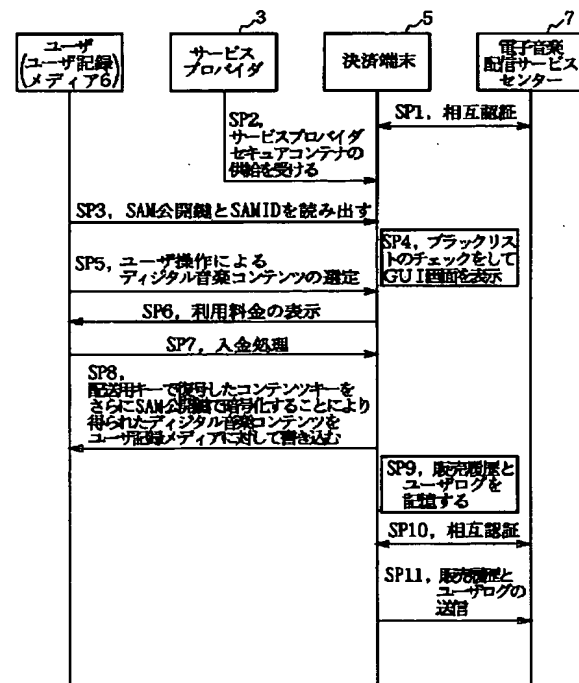


図8 買い取りでデジタル音楽コンテンツをオフライン購入するときの決済シーケンス

【図9】

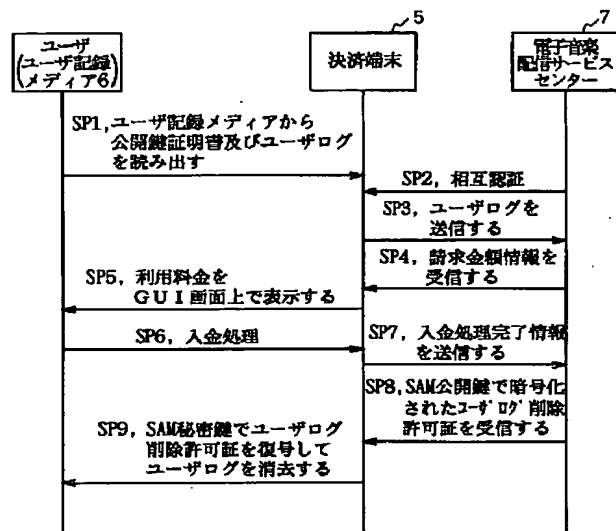


図9 デジタル音楽コンテンツをオンライン購入するときのユーザログを用いた決済シーケンス

フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テ-マ-ド' (参考)

H 0 4 L 9/00

6 7 3 B

G 0 6 F 15/30

L

Fターム(参考) 5B049 AA05 BB11 CC05 CC36 DD05
 EE03 FF02 FF03 FF04 FF06
 FF08 FF09 GG04 GG07 GG10
 5B055 BB11 CB09 EE02 EE04 EE17
 EE27 LL07 PA02 PA34 PA38
 5D044 AB03 BC01 CC04 DE49 EF05
 FG18 GK17 HL02
 5J104 AA07 KA01 KA15 MA02 NA38
 PA07 PA10